

Decentralized Trust System

Delegable AuthZ & AuthN with multiple* Authorities



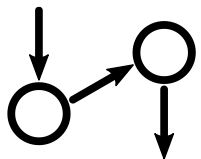
P3KI

Current Challenge



Permission & Trust Islands

Global shipping has many players, no one trusts everyone. Brokers and intermediaries are common.



Offline & Intermittent Connectivity

Relying on active third parties for verification is fragile.

P3KI Approach

Flexible Web-of-Trust & Precise Trust Anchors

Tightly scoped permission delegation on top your identity network.

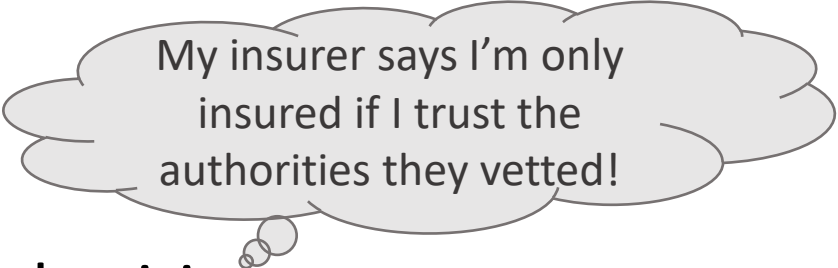
Fully Offline Capable

Verification of permissions and relationships without active 3rd parties. Made for store & forward networking. Support for non-IP networks.

1st Idea

Decentralized Identities: “The OGT”

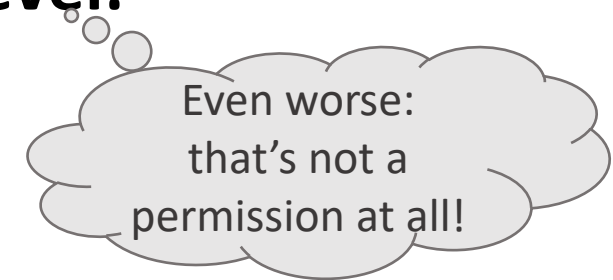
- **Handles exactly one task**
“Who to trust with MCP identities?”
- **The twist**
MCC doesn't want to be the authority, no one will
- **Solution**
 - 1) Resist urge, don't use blockchain
 - 2) Everyone can claim to be an authority
 - 3) Trusted peers attest those they deem legit authorities



My insurer says I'm only insured if I trust the authorities they vetted!

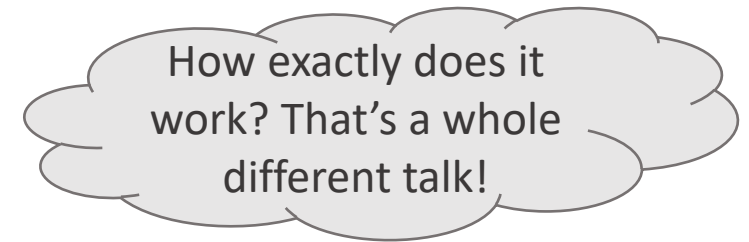
Why should we do more?

- Identity is nice, but have you thought of **permission delegation**?
Limiting what someone can do once trusted **is essential!**
Especially in a decentralized scenario!
- **Classic PKIs** (“certificates”) have only **one permission level**:
“This is one of us!”
- **Classic PKI is messy** when it comes to **revocations**
It’s effectively online only and centralized (s. CRL/OCSP)



P3KI Decentralized Trust System

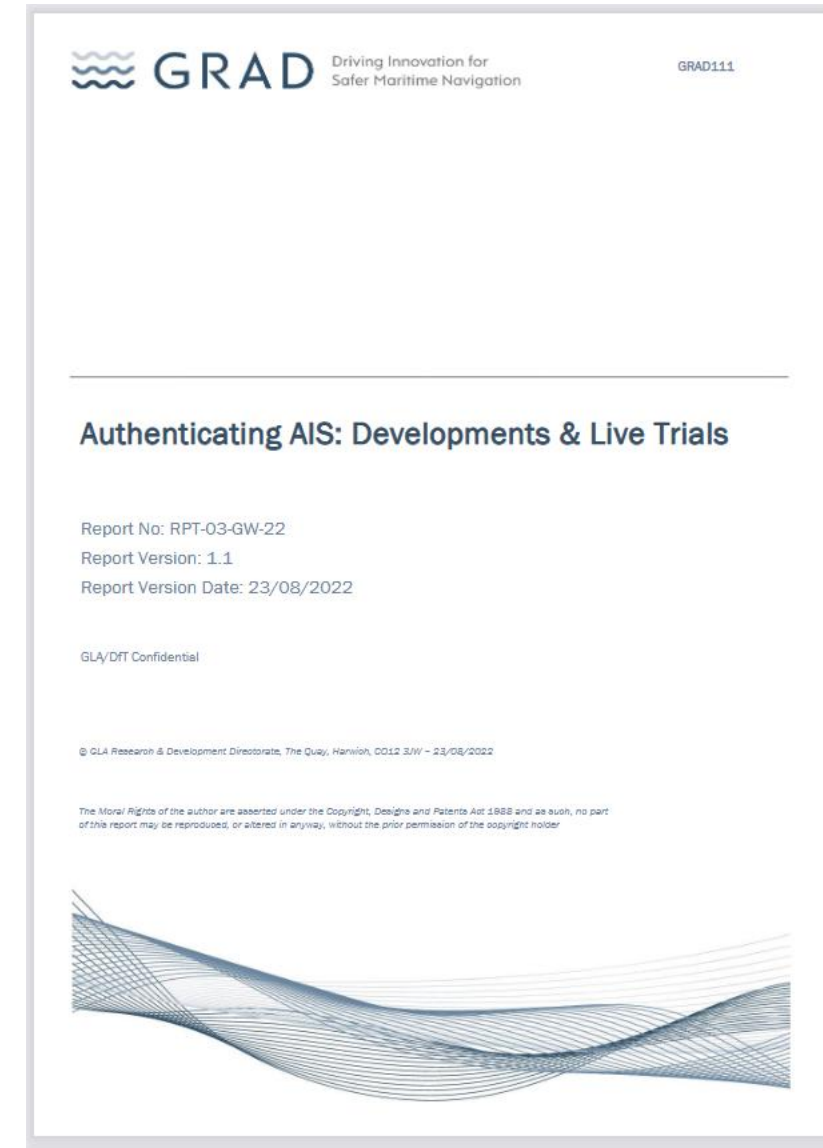
- **Permissions, not identity management**
It's what you can do, not who you are.
- **Precise delegation semantics**
You're allowed to do something;
have someone do it (or parts of it) for you.
- **Independence from central infrastructure**
Even for revocations!
Use it while it's there, though.
- **Work *together with* the classic PKI**
MCP identity certificates provide key material for signing delegations!



Application to GRAD Cork Hole Test

Excellent work adding security to V-AtoNs by GLA/GRAD

- **Danger: Governance Overhead**
Global rollout will be an organizational issue, not a technical one
- **How to add the decentralized trust system?**
No changes needed on AIS level on top of GRAD's work. Changes are purely in software.
- **What do we gain?**
Security (e.g., location spoofing protection, location bound GNSS, role/type impersonation protection, ...)
Governance flexibility
Resilience even if parts become non-operational



What do we want for the Trust System?

Limit what can be done across multiple dimensions.

- **Area**

Buoy supposed to be in the Pacific should not report data for the North Sea or vice versa

- **Type/Role**

A fixed light should not report as a floating AtoN.

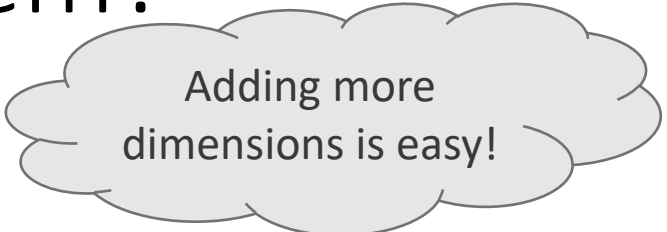
A harbor should not identify as a country.

The captain is not the ship.

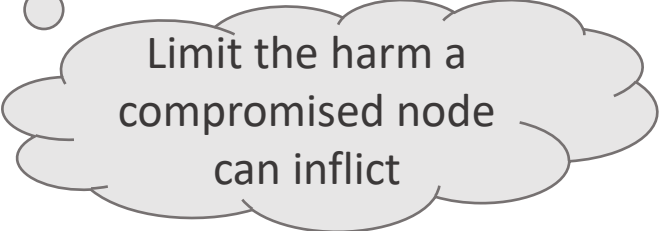
A weather report is not a cargo manifest.

- **Stage**

Test deployments should never interfere with actual navigation tasks!



Adding more dimensions is easy!

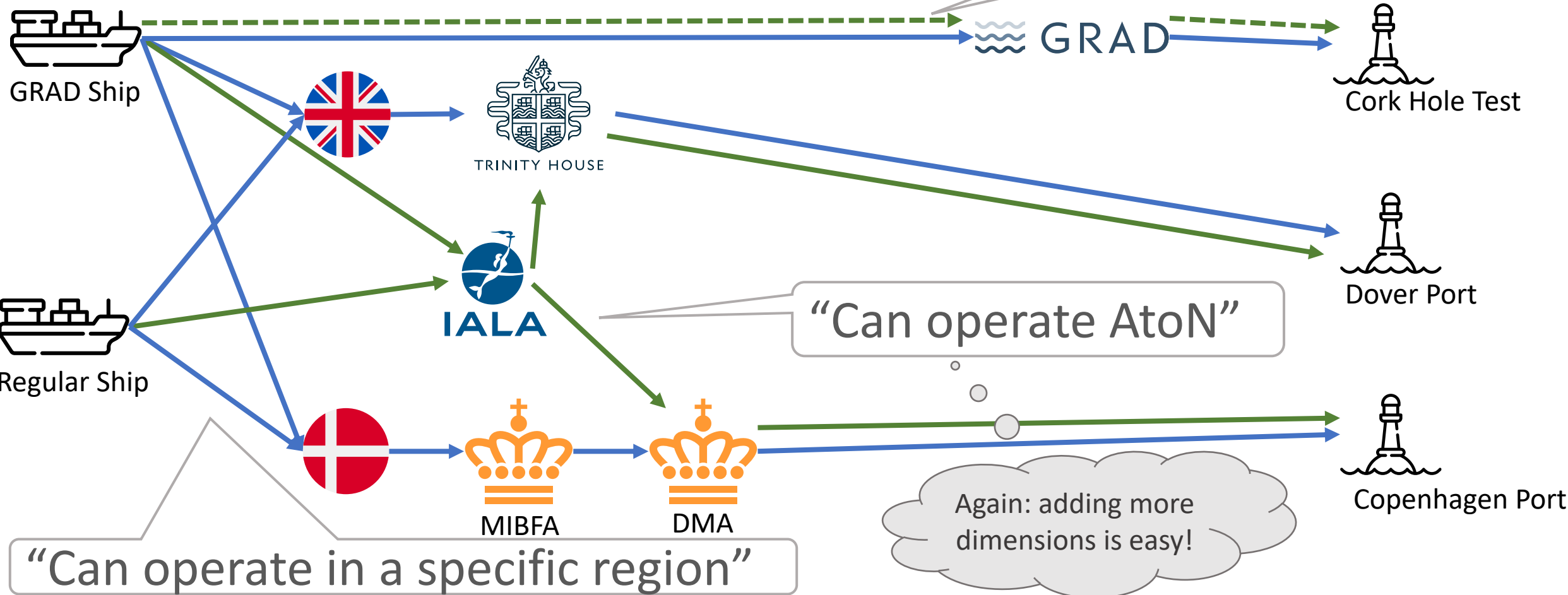


Limit the harm a compromised node can inflict

What do we want for the Trust System?

Allow flexibility in trust model and anchors

“Just testing!”



Policy Language (simplified)

stage:{**prod**}
stage:{**test**}

• **EXPR := (OLC, TYPE, STAGE)**

Plus Codes

olc:**9F7JPJ56+JHF**
olc:**9F7JPJ56+**
olc:**9F7J**

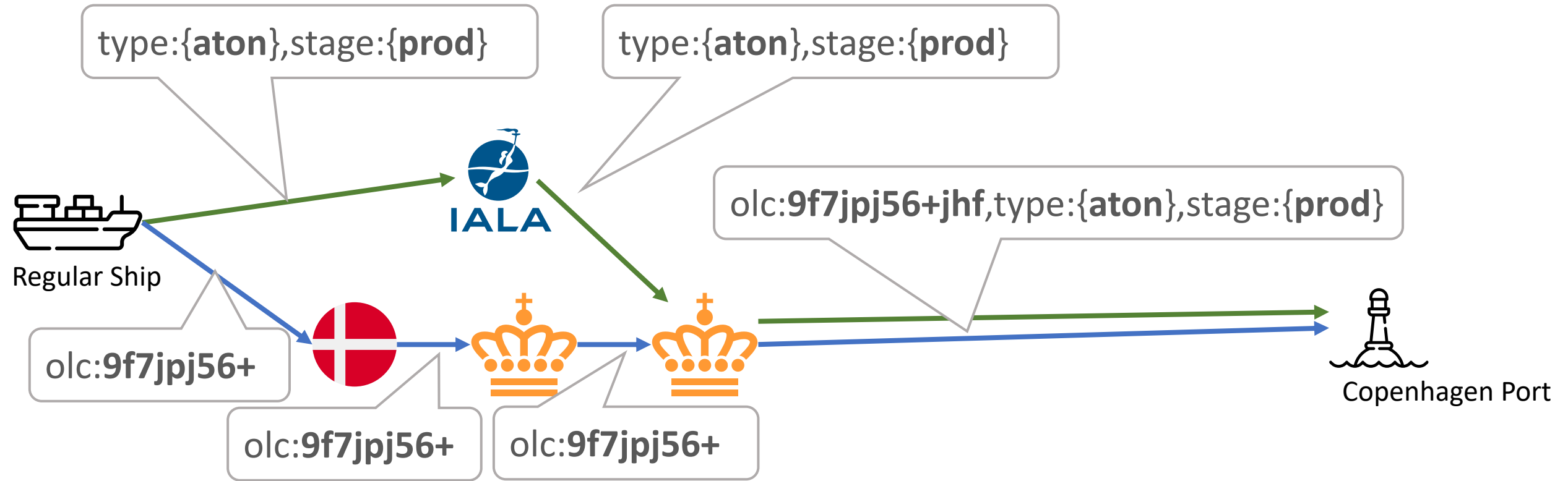
type:{**aton.fixed.light.sectors**}
type:{**aton.fixed.beacon.cardinal.n**}
type:{**aton.floating.danger**}
type:{**vessel**}
type:{**person**}
...

Production-stage fixed light at Copenhagen port:
olc:**9F7JPJ56+JHF**,type:{**aton.fixed.light**},stage:{**prod**}

Policy Example . . .

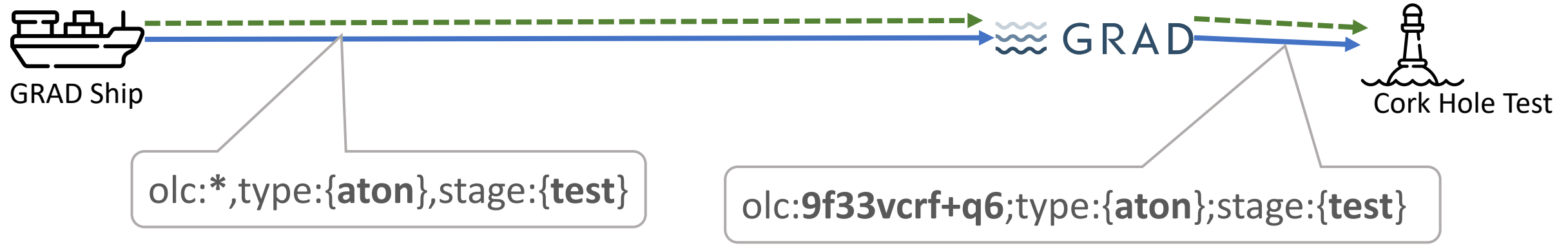
Policies define context to frame trust between identities.

A production AtoN at Copenhagen port



Policy Example

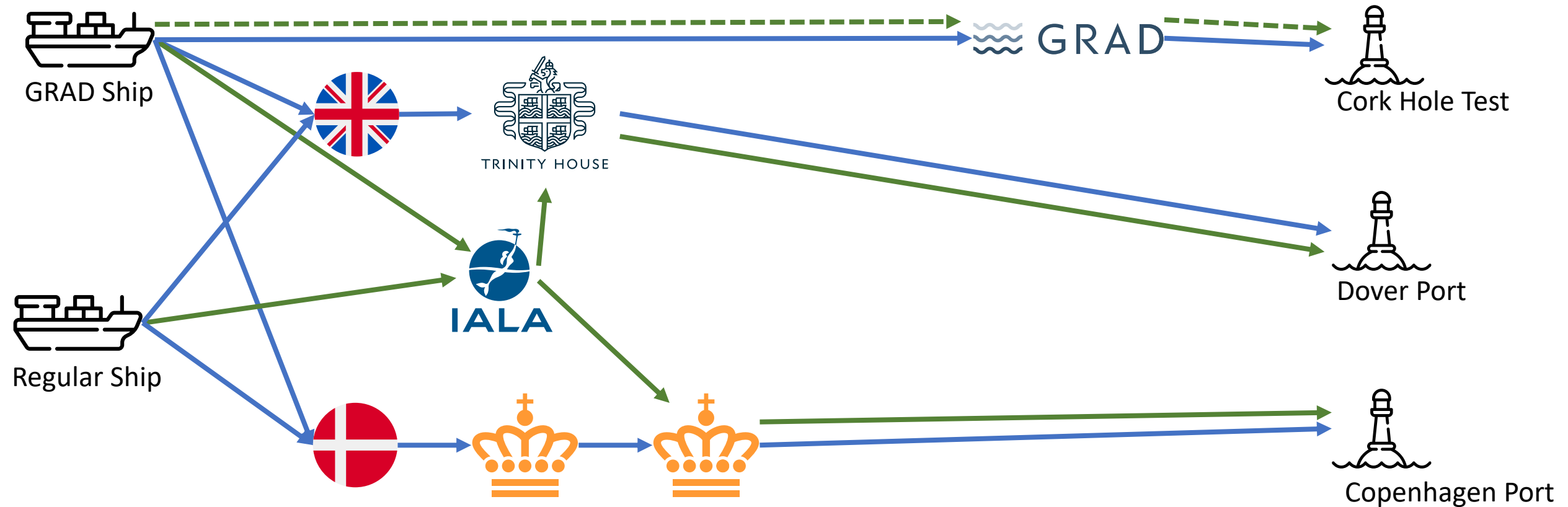
Our own boat trusts our own test deployment



What else can we do?

- **Brokers and Intermediaries**
Companies, insurers, countries, institutions, etc are easy to add
- **Authorize and authenticate arbitrary parties and operations**
Who to fetch navigational updates from?
Am I really talking to a port authority?
Verify attestations to cargo documentation
Authorize last minute relief personnel
Many more
- **Remember, all this works fully offline!**

Demo Time!



Q&A



Gregor Jehle

gregor@p3ki.com

+4915786882567

PGP: 0x2C5996E1DBD36223

Try it Yourself!



AtoN



Ship